

IN THE ABSTRACT:

Please amend the Abstract on Page 38 as follows:

USING TRUSTED CO-SERVERS TO ENHANCE
SECURITY OF WEB INTERACTION

ABSTRACT

A trusted co-server, and a method of using a trusted co-server, for a service provider. The co-server executes a program such that: for multiple parties P_0 - P_n (where P_0 is said co-server), each party P_i may (optionally) provide input I_i , and then said co-server carries out N functions: F_i ($i_0...I_n$) describes what the co-server returns to party P_i . The preferred embodiment of the invention raises the trust level of the computation and data storage at the ~~server~~ server. For instance, this invention may be witness to authenticity of certain data coming back to the client. This data can include assertions from the trusted co-server about the server content and configuration. The invention, also, can provide privacy of data going back to the server, by keeping it encrypted between the client and the co-server, and then re-encrypting it before inserting it into the server. With this invention, the user can trust the integrity of the computation occurring at the co-server---even if the server operator might be motivated to subvert it. The co-server also provides a trusted haven for computation relevant to third parties who may also have an interest in the client-server interaction.